# Friede den Telegram-Kanälen

Sebastian J. Golla 2021-02-10T10:53:05

Das Bundesministerium der Justiz (BMJV) plant, einen neuen Straftatbestand für die Verbreitung von „Feindeslisten“ vorzuschlagen. Der Entwurf erscheint nicht gut durchdacht, liefert aber einen Anstoß für Überlegungen zu einer umfassenden Reform des Datenschutzstrafrechts.

## Virtueller Austausch, reelle Auswirkungen

Das seit etwa zwei Jahren diskutierte Vorhaben hat seinen Ursprung vor allem in der Verbreitung von Listen politischer Gegner in rechtsextremen Kreisen. Der Umgang mit derartigen Listen kann dazu dienen, die Betroffenen gezielt zu verunsichern. Die Verbreitung von personenbezogenen Daten wie Anschriften und Telefonnummern öffnet im virtuellen Raum ein Tor zu möglichen reellen Gefahren, die von Drohbriefen bis zu Anschlägen auf Leib oder Leben reichen können. Dem will das BMJV mit einem Straftatbestand entgegenwirken, der wir folgt lauten soll:

> § 126a StGB
>
> Gefährdende Veröffentlichung personenbezogener Daten
>
> (1) Wer öffentlich, in einer Versammlung oder durch Verbreiten eines Inhalts (§ 11 Absatz 3) personenbezogene Daten einer anderen Person in einer Art und Weise verbreitet, die geeignet ist, diese Person oder eine ihr nahestehende Person der Gefahr eines gegen sie gerichteten Verbrechens oder einer sonstigen rechtswidrigen Tat gegen die sexuelle Selbstbestimmung, die körperliche Unversehrtheit, die persönliche Freiheit oder gegen eine Sache von bedeutendem Wert auszusetzen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
>
> (2) Handelt es sich um nicht allgemein zugängliche Daten, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.

## Der öffentliche Frieden in Messenger-Gruppen

Bemerkenswert ist zunächst, dass der Tatbestand vorrangig den öffentlichen Frieden schützen soll und nicht etwa die Freiheit der von derartigen Verbreitungen Betroffenen. Dies zeigt auch die Nähe zu § 126 StGB, der die Störung des öffentlichen Friedens durch Androhung von Straftaten unter Strafe stellt.

Zugleich soll sich die Strafbarkeit auf Räume beziehen, in denen Öffentlichkeit und Privatheit verschwimmen. So soll nach der (unveröffentlichten, dem Verfassungsblog und dem Autor vorliegenden) Begründung auch die Verbreitung von Daten in Gruppen bei Messengern wie WhatsApp oder Telegram strafbar sein, selbst

wenn diese nur geschlossenen Nutzerkreisen zugänglich sind. Bei einer größeren Mitgliederzahl ließe sich dies unter das „Verbreiten eines Inhalts“ fassen. Fraglos kann die Verbreitung von Informationen in mitgliederstarken geschlossenen Kanälen gefährlich sein. Es erscheint aber schief, diese stark fragmentierten und teils obskuren Kommunikationsräume im Namen des öffentlichen Friedens ins Visier des Strafrecht zu nehmen.

Dazu geht es dem Entwurf augenscheinlich eher um die Verbreitung von Informationen als um deren Veröffentlichung. Das zeigt die in Abs. 2 vorgesehene Qualifikation, die das Verbreiten von „nicht allgemein zugänglichen“ Daten unter eine höhere Strafe stellt. Im Umkehrschluss bedeutet dies, dass eine Strafbarkeit nach § 126a Abs. 1 StGB-E auch dann möglich ist, wenn Daten weitergegeben werden, die bereits öffentlich bekannt sind – so etwa bei aus einem Impressum entnommenen Adressdaten.

## Einschüchterung durch den Schutz vor Einschüchterung

Damit bezieht sich der Entwurf weniger auf klassische Fälle des „Doxing“ oder Indiskretionen als auf die Gefahren der unkontrollierten Weitergabe von Daten. Um die Verbreitung strafbar werden zu lassen, muss keine Folgestraftat begangen werden oder gar eine konkrete Gefahr für den Betroffenen entstehen. Ausreichend ist, dass die Verbreitung konkret geeignet ist, den Betroffenen der Gefahr bestimmter Straftaten auszusetzen. Darunter fallen neben Nötigungen und Bedrohungen auch Sachbeschädigungen gegen Sachen von einem bedeutenden Wert, der sich schon ab 750 Euro annehmen lässt.

Wann die nötige konkrete Eignung zu einer Gefährdung besteht, ist dabei unklar. Die Begründung des Entwurfes führt hierfür unter anderem den Kontext der Verbreitung (etwa auf extremistisch ausgerichteten) Internetseiten, Bezüge zu Straftaten bei der Verbreitung und die Anonymität des Verbreitenden an. Rechtssicherheit geben diese Kriterien nicht. Der Schluss von der Anonymität des potentiellen Täters auf die Gefährlichkeit des Inhalts ist so allgemein nicht plausibel. Offen bleibt auch, nach welchen Kriterien die Verbreitung von Informationen in Medien mit Breitenwirkung geeignet sein kann, die Gefahr von Straftaten auszulösen.

Führt etwa ein Dortmunder Lokaljournalist, der über das neue Luxusauto eines Schalker Profis berichtet, durch die Verbreitung personenbezogener Daten die Gefahr einer Sachbeschädigung herbei? Auch wenn eine strafrechtliche Verurteilung in derartigen Fällen unwahrscheinlich ist, sind die Einschüchterungseffekte nicht zu unterschätzen, die aus dem gewollten strafrechtlichen Schutz vor Einschüchterung folgen könnten. Sie wiegen besonders schwer, wenn die Verfolgung der eigentlich bedrohlichen Verhaltensweisen (wie der Hetze in schwer zugänglich Kanälen) praktisch kaum gelingt. Dann stehen geringen Erträgen der Verschärfung des Strafrechts hohe Freiheitsrisiken entgegen.

# Plädoyer für ein neues Datenschutzstrafrecht

So verständlich das Anliegen des neuen Tatbestandes ist – seine Ausgestaltung erscheint verfehlt. Der Entwurf bietet jedoch Anlass, über grundlegendere strafrechtliche Reformen nachzudenken. So ist die Veröffentlichung von personenbezogenen Daten bereits strafbar, wenn sie mit Schädigungsabsicht geschieht (§ 42 Abs. 1 Nr. 1 BDSG). Die Schädigungsabsicht lässt sich auch dann annehmen, wenn Täter*innen ihre Opfer einschüchtern wollen (LG Aachen, Urteil vom 18.02.2011 – 71 Ns-504 Js). Auch wenn der Nachweis des subjektiven Elements in manchen Fällen schwierig sein mag, er ist gegenüber der unklaren Anknüpfung an die Eignung zur Gefährdung einer Person vorzugswürdig.

Das Datenschutzstrafrecht, das das BDSG regelt, wird in der Praxis allerdings kaum wahrgenommen und angewandt. Eine Ausnahme bildet etwa die Verurteilung eines jungen Hackers, der im Winter 2018/2019 mit der Veröffentlichung von Daten über Politiker*innen und Prominente für Aufsehen sorgte. Gründe für das Schattendasein des Datenschutzstrafrechts sind unter anderem die Unbestimmtheit der Regelungen, das Antragserfordernis und der Standort außerhalb des StGB.

Betrachtet man die vielfältigen Risiken, die vom Missbrauch personenbezogener Daten in der digitalisierten Welt ausgehen, wird das der Materie nicht gerecht. Es wäre sinnvoll, das Datenschutzstrafrecht in das StGB zu integrieren und seine Regelungen mit Blick auf bestimmte Risiken zu schärfen. Im gleichen Zug ließen sich auch weitere Straftatbestände anpassen und modernisieren (ähnlich *Kubiciel/ Großmann*, NJW 2019, 1050 (1055)). So könnte an die Stelle eines kontinuierlich punktuell verschlimmbesserten und dadurch destabilisierten IT-Strafrechts ein kohärentes System treten, das aktuelle Gefährdungen berücksichtigt und gleichzeitig die „ultima ratio“-Funktion des Strafrechts wahrt.

---